¿CÓMO EVITAR CIBERATAQUES EN LAS MIPYMES COLOMBIANAS?

A. Londoño Pamplona[1], C. Quintero[1] y K.I. Medina Fonseca[1]

[1] Semillero de investigación SIPI, Centro De Servicios y Gestión Empresarial, Servicio Nacional de Aprendizaje SENA. Medellín, Colombia.

londonoalejandra400@gmail.com; camilaquintero723@gmail.com; karimedi125@gmail.com

Palabras clave: Ciberataques, Mipymes, Sistemas de seguridad.

RESUMEN

En este artículo de revisión documental, se aborda un asunto poco conocido pero lastimosamente bastante común, más aún en la contingencia por el Covid 19, y es el relacionado con los ciberataques, los cuales se presentan mayormente en micro, pequeñas y medianas empresas, ya que los atacantes se aprovechan de los pocos sistemas de seguridad que en estas entidades se manejan y de sus escasas medidas preventivas. De ahí, que este artículo aborde la importancia de implementar sistemas de seguridad en las mipymes colombianas, partiendo de dos temas fundamentales, el primero de ellos, la caracterización de los principales ciberataques que se presentan en este segmento de empresas, y el segundo, las medidas preventivas que se hace necesario adoptar para evitar estos ciberataques de manera oportuna.

01 INTRODUCCIÓN

La pandemia por el Covid 19 provocó el acelerado crecimiento de la actividad digital del sector productivo colombiano y todas las empresas, desde la más pequeña hasta la más grande, pueden llegar a ser afectadas por esta realidad, pues lo que anteriormente era considerado un "plus" para aumento de productividad y utilidades, hoy en realidad es un requisito fundamental de supervivencia, debiendo las mipymes dotarse, no solo de conexiones rápidas y estables y de dispositivos sofisticados, sino también de sólidos esquemas de ciberseguridad [1], pues solo a pocos días de declararse la pandemia por el Covid 19, más exactamente durante el primer semestre del año 2020, se aumentaron los delitos informáticos en Colombia en un 59% respecto al mismo semestre del año 2019, según lo reveló el Centro Cibernético de la Policía Nacional [2].

Esta ciberseguridad se clama como indispensable para todas las empresas con operaciones digitales, ya que es conocido que la proliferación de las tecnologías, trae indefectiblemente ataques informáticos y nuevos ciberdelitos [3], lo cual repercutirá negativamente en el quehacer productivo de estas mipymes que, en su mayoría, cuentan con poca o nula preparación para enfrentar las consecuencias.
Incluso, estudios han afirmado que un gran porcentaje de las mipymes del país, quedan imposibilitadas para continuar su actividad empresarial por más de un semestre, luego de recibir un ciberataque considerable [4].

Según un estudio realizado por el BID, MINTIC y la OEA, que analiza el efecto de los ataques de seguridad digital, los empresarios colombianos afirman que dentro de los principales factores que afectarían su capacidad de afrontar la seguridad digital, están la falta de conocimiento específico sobre el tema, sumado a ello, el poco dinero destinado a esta área, seguido de la baja conciencia por parte de los empleados [5].

De los factores mencionados, los dos primeros, es decir, el contar con personal dedicado de manera exclusiva a temas de ciberseguridad en las mipymes y el escaso presupuesto para invertir en acciones preventivas, hacen que estas pequeñas empresas vean escasas posibilidades de enfrentar el potencial riesgo, pues es conocido que la crisis económica por el Covid 19 afectó de manera contundente a las mipymes del país, las cuales fueron especialmente vulnerables, ya que no disponían de los medios necesarios para adaptarse a un fuerte choque externo como el recibido con ocasión de la pandemia, el cual provocó alteración en las obligaciones de este segmento empresarial [6].

En este contexto, se hace necesario buscar alternativas coherentes con la actual situación financiera de este grupo de pequeños empresarios, brindándoles algunas propuestas que permitan la prevención de un posible ataque cibernético, pero sin sacrificar el escaso presupuesto disponible para invertir en la actual reactivación de su actividad comercial.

Es así como esta investigación pretende, en un primer momento, caracterizar los principales ciberataques que reciben las empresas colombianas para, posteriormente, generar una propuesta que permita la sensibilización del talento humano de estas mipymes respecto a las acciones que se pueden dar para evitar y enfrentar este flagelo en el ámbito digital, dando así respuesta al tercer factor mencionado como incidente en la capacidad de afrontar la seguridad digital, el cual se refería al escaso conocimiento que se tiene del tema dentro de una empresa.

02 METODOLOGÍA

Este trabajo acude a la investigación cualitativa de tipo documental, la cual implica trabajar directa o indirectamente sobre la base de textos o documentos, lo que hace que se asocie con investigación bibliográfica; aunque en realidad, en la investigación documental, el concepto de documento es mucho más amplio, pues incluye no solo documentos escritos, sino también, diapositivas, videos y películas que aporten información relevante a la investigación.

Para el desarrollo del presente artículo se analizan 19 documentos, nacionales e internacionales, publicados entre el año 2017 a 2021, los cuales abordan el tema de los ciberataques y sus modalidades preventivas en el contexto empresarial; algunos de ellos, se enmarcan específicamente en las tendencias del cibercrimen en las empresas colombianas, lo que nutre, de manera pertinente, la propuesta planteada en este artículo.

Los documentos fueron recuperados de diferentes repositorios digitales, privilegiando aquellos de índole académica. También se acude a medios informativos masivos, los cuales, a partir de un periodismo de investigación, ofrecen información relevante y actualizada, y finalmente, se extraen algunos apartes de informes expedidos por entidades oficiales, como el BID, MINTIC, OEA, entre otros, los cuales ostentan características como la imparcialidad y confiabilidad.

Se excluyen documentos con enfoque exclusivamente técnico en el área de delitos informáticos y sus respectivos sistemas de seguridad, pues, aunque aborden de manera objetiva la temática, abandonan la simplicidad en la comprensión necesaria para el público objeto de la propuesta esbozada en este artículo.

Es de anotar, que, respecto a la información sobre medidas preventivas de los ciberataques, solo se incluye aquella cuya adopción es pertinente a las condiciones actuales de las mipymes colombianas, las cuales, además de poseer limitados activos tecnológicos, carecen de recursos económicos, humanos y técnicos suficientes para la implementación de sistemas de seguridad refinados.

03 RESULTADOS Y DISCUSIONES

Alrededor de marzo del 2020, a causa de la pandemia por el Covid 19, se hizo necesario que los ciudadanos continuaran con el desarrollo de sus actividades a pesar del confinamiento obligatorio, y por ello, empezaron a depender en gran medida de la conectividad diaria, lo cual desató una cantidad de amenazas cibernéticas. Estos delincuentes aprovecharon los vacíos que tenían los usuarios, además del pánico colectivo que se vivía. [7]

Las micro, pequeñas y medianas empresas colombianas no fueron ajenas a tales ciberataques, pues en realidad, eran las que menos esquemas de seguridad tenían y las que tuvieron menor espacio y capacidad económica para formar a sus trabajadores en la materia.

Por ello, la importancia de destacar los principales ciberataques que se desataron en el contexto de la pandemia, para finalmente, definir un protocolo preventivo enfocado a las circunstancias particulares de estas pequeñas empresas.

3.1 PRINCIPALES CIBERATAQUES EN EMPRESAS

Luego de analizar la información recolectada, se puede inferir que los principales ciberataques que sufren las empresas en la actualidad, son los siguientes:

a. Phishing:
Consiste en el envío de correos electrónicos a empresas, en las que el remitente se hace pasar por fuente confiable para así poder obtener información confidencial de la víctima, luego realizan algún tipo de fraude, ya sea para beneficio propio o de terceros, vendiendo datos o información robada. Para realizar esto, incluyen un enlace, que al hacer clic, lleva al usuario a páginas web falsificadas. El usuario, pensando que está en un sitio web de confianza, ingresa toda la información solicitada, entregándosela a estafadores. [8]

El phishing toma datos personales o corporativos, como direcciones de correos electrónicos, números de documentos de identificación o datos de localización. También puede robar credenciales de acceso a redes sociales y a correos electrónicos, incluso tomar información de liquidez y flujo de caja de una empresa [8].

Tipos de phishing: [8]
- Spear phishing: Este tipo de phishing está dirigido a grupos pequeños, esto permite que las campañas sean más personificadas y con un mayor número de víctimas.
- Whaling: Se dirige a niveles más grandes, como ejecutivos o empresariales, sus preferencias son los de más altos niveles como los CEOS. Las probabilidades de que caigan en este tipo de phishing no son muchas, en los pocos casos caen por algo “especial”.
- Cloning: Este tipo de phishing utiliza la suplantación de identidad de correos legítimos, el cual es entregado al buzón del usuario, de esa manera utilizan para crear un correo clonado.
- Phishing con geolocalización: Este tipo de phishing es utilizado para permitir o denegar el acceso a sitios web falsos de los usuarios de cierto país, por medio de la dirección IP o un servidor proxy.

Fases del Phishing:
- Planificación y configuración: Seleccionan la empresa a la cual van a atacar, con el objetivo de obtener detalles básicos. Luego, se diseñan los ataques que entrarán en acción por medio de sitios web, correos electrónicos u otros, incluyendo enlaces maliciosos. Los cuales pueden redirigir al afectado a un sitio fraudulento.
- Agresión de Phishing: Los ciber atacantes envían correos electrónicos falsos, disfrazados de emails de empresas que gozan de buena reputación y solicitan información

confidencial, indicando que es urgente actualizar base de datos o actualizar sus registros, e incitan a entrar a un sitio malicioso.
- Introducción: Al dar clic en el enlace malicioso, un programa malintencionado se introduce de forma involuntaria en el dispositivo tecnológico, lo que da paso al atacante para que este pueda visualizar la información, cambiar configuración y derechos de acceso.
- Recopilación de datos: Los atacantes empiezan a extraer los datos requeridos de la empresa, lo que podría conducir a pérdidas financieras para la víctima.
- Extracción: Posteriormente, el atacante borra todas las evidencias del sistema.

b. Malware:

Son una modalidad de ataques bastante astutos y maliciosos, los cuales se emplean a fin de causar daño al hardware, software y, finalmente, al usuario. Quienes utilizan este tipo de ataques pueden sustraer información valiosa; habitualmente buscan encontrar información personal, como registros de transacciones financieras o inversiones, bases de datos de clientes, documentación técnica, entre otros. También pueden conseguir dinero, amenazando al dueño de la información con revelar información privada. Finalmente, puede hackear un equipo y tener el dominio total de este para causar daño [9].

Según el modo de operar de la persona y del ataque que emplea, el malware puede quedar en una categoría, esta cambia según el caso particular que se presente. Esta modalidad causa mucho daño a nivel personal y a nivel empresarial, por tal motivo siempre se recomienda estar muy al tanto de las actualizaciones del software antimalware a fin de tener una protección constante y apropiada en el equipo. [9]

En Colombia, la infección por malware sigue en crecimiento, incluso en el año 2018, solo 99 empresas reportaron casos de malware en sus infraestructuras, mientras que al año 2019, ya se hablaba de 705 casos registrados y de ellos, la mayoría eran pequeñas y medianas empresas. Y obviamente, con ocasión de la pandemia, las cifras siguen en crecimiento [10].

Dentro de la categoría de malware se encuentran los virus, los cuales son creados para copiarse a sí mismos y difundirse a una cantidad amplia de dispositivos, modificando o eliminando archivos guardados en el equipo, al tiempo que pueden dañar un sistema, eliminando o corrompiendo datos esenciales para su adecuado funcionamiento.

Dentro de esta categoría del malware también se encuentra el Adware, el cual es un software malicioso que muestra de manera masiva anuncios no deseados con el fin de recopilar información sobre la actividad de la empresa. El spyware también hace parte de la categoría de malware, y son los que se instalan en los equipos de las empresas para recopilar información para finalmente compartirla con un usuario remoto.

Los troyanos también se encuentran dentro de los malware y suelen camuflarse con el ropaje de un software legítimo, con la intención de infectar equipos en las empresas, pudiendo controlar los equipos, robar datos, introducir otros softwares maliciosos y propagarse a otros dispositivos. [9].

Otra vertiente es el Ransomware, en la que el atacante cifra la información del usuario y luego pide dinero para su rescate, casi siempre, exigiendo pago con bitcoin para conservar su identidad, pudiendo afectar desde un solo usuario conectado a internet hasta una red de computadoras conectadas a una LAN en una empresa, ocasionando interrupción en las funciones, pérdidas monetarias e incluso, afectando la reputación empresarial [11].

Finalmente, el Spyware, cuya denominación se compone de las palabras espía y software, trabaja bajo el mismo mecanismo, obteniendo datos personales y sensibles como contraseñas, credenciales de inicio de sesión e información bancaria [12].

c. Fake news o noticias falsas:

Son historias o anuncios sensacionalistas que se comparten en redes sociales con la finalidad de involucrar emocionalmente a los lectores, captando su atención y llevando a sus creadores a obtener rentabilidad vía clics y viralización. Otra de sus finalidades, es desprestigiar a personajes públicos o empresas. También buscan que los usuarios descarguen archivos adjuntos o den clic en enlaces con virus informáticos, los cuales pueden robar información financiera, datos personales y contraseñas. [13]

Esta palabra empezó a tener gran importancia cuando se dieron las elecciones de EE. UU del 2016 para elegir al presidente, cuando los medios empezaron a percatarse de algunas noticias falsas que se difundieron rápidamente por la internet, con estas historias inventadas tienen un sentido estricto que tienen motivaciones económicas, políticas o un poco de ambas. Como hacen pública la información, pagan publicidad para que ese artículo sea visto por muchas personas ya que lo montan a páginas donde tienen muchas visualizaciones y hacen que estas noticias sean más creíbles. [13]

Es de anotar que una noticia falsa tiene el potencial de compartirse 6 veces más rápido que una real y con internet pueden llegar a unas audiencias más amplias que si estuviera en el contexto tradicional. Es de anotar que esas publicaciones tradicionales, realizadas en prensa, radio o televisión, poseían sistemas internos para controlar la veracidad de la información antes de ser promulgada, a diferencia de los nacientes canales digitales, en los cuales se hace imposible controlar la información [14].
Esta situación es preocupante para las mipymes colombianas, pues un estudio de la firma rusa Kaspersky, indicó que Colombia ostenta uno de los lugares más altos en la clasificación de países latinoamericanos que más consume noticias falsas, con un 73% de participación. Además, esa comunidad latina en un 16% desconoce por completo el

término de “noticias falsas” o “fake news”. [15]

Estas noticias falsas pueden causar grandes perjuicios económicos para las empresas, aunque hay quienes estiman que hay otros riesgos considerables, por ejemplo, un estudio realizado por Estudio de comunicación en colaboración con Servimedia, estableció que el 85.5% de los encuestados cree que el riesgo reputacional es el perjuicio más relevante dentro de esta problemática. [16]

3.2 PROPUESTA A LAS MIPYMES COLOMBIANAS PARA EVITAR LOS CIBERATAQUES

Los ciberataques actualmente son más comunes que nunca y las mipymes (micro, pequeñas y medianas empresas) no se libran de estos, pues cualquier empresa que manipule o almacene información se encuentra propenso a sufrir un ciberataque, importante generar medidas de protección para la empresa, por esto a continuación se definen algunas de ellas, las cuales pueden ser un apoyo para la empresa [17]:

a. Usar autenticación multifactor:
Este sistema de seguridad lo que busca es generar varias contraseñas para acceder a la información, pues no es suficiente con que los empleados solo utilicen una para autorizar el ingreso a información valiosa, al tener habilitado este sistema será más difícil que el atacante acceda a los sistemas de la empresa puesto que la seguridad de la información aumentará.

b. Contar con controles de acceso sólidos:
Lo que permiten estos controles es generar una actualización inmediata al finalizar la jornada laboral o al tomar un receso, pues quienes operan en la empresa anulan el acceso a los equipos, logrando así que ninguna otra persona tenga acceso a la información valiosa que allí se encuentra.

c. Compromiso de seguridad a terceros:
Se debe comprender la seguridad que se debe tener con terceros, en caso de que un cliente, un proveedor, un trabajador, un banco... requiera acceder al sistema de la empresa es primordial conocer los riesgos y asegurar una mayor responsabilidad.

d. Capacitar a los empleados sobre seguridad:
Se debe proporcionar entrenamiento, tanto a los empleados que inician en la empresa como a los que llevan ya un tiempo, de forma regular, preferiblemente cada año; esto es importante porque cuando el personal se concientiza de los peligros que se pueden encontrar en la web, va a estar más preparado para defenderse de un ciberataque.

e. Generar copias de seguridad:
A causa de los ataques cibernéticos o por un problema informático, mucha información importante de la empresa, como datos de clientes, trabajos en proceso, información legal, etc., pueden borrarse o dañarse; una solución para evitar esto, y trabajar de forma segura, es realizar copias de seguridad de forma periódica para que la información crucial se preserve.

f. Estar al tanto de las actualizaciones de los software empresariales:
Si se quiere que la información de la empresa esté segura, se deben ejecutar las actualizaciones siempre que el sistema lo requiera; aunque estas actualizaciones sean constantes valdrá la pena realizarlas, pues de no hacerlas el sistema no podrá defenderse de las posibles amenazas a la seguridad que puedan surgir.

g. Instalar un cortafuegos (firewall) y un antivirus en todos los equipos de la empresa:
El firewall va a prevenir y proteger a nuestra red privada de intrusiones o ataques de otras redes, bloqueando el acceso, y el antivirus, detecta la presencia de un virus informático en una computadora y lo elimina; cabe aclarar que, aunque estas herramientas son bastante útiles y eficaces, no son suficientes para proteger a la empresa, se deben tener en cuenta también las sugerencias mencionadas anteriormente.

3.3 PROPUESTA AL EQUIPO HUMANO DE LAS MIPYMES COLOMBIANAS PARA EVITAR LOS CIBERATAQUES

a. Verificar que los dispositivos que se usen cuenten con un software antivirus, ya que ellos realizan actualizaciones automáticas que permiten la detección regular de nuevos virus y amenazas, además analizan los correos electrónicos, evitando que contengan enlaces o archivos maliciosos.

b. Solicitar a la empresa que los equipos tecnológicos que se proporcionen, cuenten con herramientas de ciberseguridad como firewall perimetral de red, servidor proxy, cifrado de punto final y escáner de vulnerabilidades, las cuales tienen el potencial de detectar posibles amenazas, bloquear accesos no autorizados y, finalmente, gestionar los puntos débiles del sistema.

c. Si se va a trabajar desde casa, es importante que los equipos cuenten con un software de monitoreo a distancia.

d. Generar conciencia es un aporte fundamental para el crecimiento de la empresa, pues en gran medida, los ciberataques se dan por no tener un conocimiento claro de los tipos de ataques que existen; los gerentes deben afianzar ese conocimiento en sus

empleados por medio de campañas de sensibilización, las cuales busquen que se comprendan los riesgos que se pueden hallar en la web y a los que se pueden enfrentar, y se sepa qué acciones deben tomarse para abordarlos de la mejor forma y también mejorar la protección de la información valiosa de la empresa. Debe existir una prioridad en la realización de estas capacitaciones, y debe haber una evaluación y una supervisión constante para evidenciar que los empleados están capacitados adecuadamente para cumplir sus responsabilidades de una forma segura. [18].

e. Aprender a identificar mensajes de phishing, y si se accede a ellos, evitar el suministro de información confidencial tanto de ellos como de la empresa, especialmente información relacionada con contraseñas, con información bancaria o financiera. Esto aplica especialmente en el relleno de formularios solicitados en correos electrónicos, páginas web e incluso en servicios de mensajería instantánea.

f. Si existe sospecha del mensaje, no se debe dar clic en la información que incluya para entrar al enlace. Primero se debe asegurar si la dirección es en realidad la que pretende ser o es sólo parecida al poner el ratón en el enlace.

g. Se sugiere analizar periódicamente el estado de cuentas bancarias, en el caso de tenerlas en algún banco en internet. Para ingresar a los sitios de internet de bancos o similares, se aconseja digitar el nombre del sitio, evitando ingresar a partir del clic en algún enlace obtenido por otro medio. Es necesario verificar que el localizador de recursos uniforme (URL) comienza por el protocolo seguro de transferencia de hipertexto (HTTPS) (con la S al final) y el navegador evidencie un símbolo de un candado, lo cual revela que es una página web segura. [19]

04 CONCLUSIONES

Se debe considerar que cualquier empresa micro, mediana o pequeña, puede ser víctima de un ciberataque, pues en todas se manipula y se almacena información, y de igual forma, al ser las que menos sistemas de seguridad poseen son las más apetecibles por los atacantes.

“El conocimiento nos hace responsables” - Ernesto ‘Che' Guevara. Si estamos al tanto de los principales ciberataques que se pueden presentar vamos a ser conscientes de las obligaciones que las mipymes deben cumplir y actuar conforme a ellas, pues generalmente los ciberataques se dan por no tener un conocimiento claro de los tipos que existen. Las principales modalidades se dan al recibir correos electrónicos haciéndose pasar por fuentes confiables, virus que atacan al software empresarial y anuncios falsos en redes sociales que al ser tan virales llegan a ser creíbles.

Las medidas de protección son elementales en una empresa, pues al aplicarlas, la seguridad de la información aumentará, se pueden generar varias contraseñas para acceder a la información, realizar copias de seguridad de forma periódica, ejecutar las actualizaciones siempre que el sistema lo requiera e instalar un cortafuego (firewall) y un antivirus en todos los equipos de la empresa, también es importante capacitar a los trabajadores, pues cuando el personal se concientiza de los peligros que se pueden encontrar en la web va a estar más preparado para defenderse y actuar de la mejor forma.

05 AGRADECIMIENTOS

Extendemos un agradecimiento al semillero de investigación SIPI del SENA Centro de servicios y gestión empresarial.

06 REFERENCIAS

[1] Henriquez, P. 2020. COVID-19: ¿Una oportunidad para la transformación digital de las pymes? Puntos sobre la i. https://blogs.iadb.org/innovacion/es/covid-19-oportunidad-transformacion-digital-pymes/

[2] Portafolio, 2020. Delitos informáticos, la otra pandemia en tiempos del coronavirus. Colombia. https://www.portafolio.co/economia/delitos-informaticos-la-otra-pandemia-en-tiempos-del-coronavirus-544642

[3] Rueda Quintero, J.A. 2020. Estudio monográfico: impacto de la técnica de ataque de phishing en Colombia durante los últimos cinco años. UNAD, Bogotá, Colombia. Página 19 https://repository.unad.edu.co/bitstream/handle/10596/38721/jaruedaq.pdf?sequence=1&isAllowed=y

[4] Policía nacional, 2020, Tendencias cibercrimen en Colombia 2019-2020. Página 34-40.
https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf
[5] BID; MINTIC Y OEA, 2017. Impacto de los Incidentes de Seguridad Digital en Colombia.
https://publications.iadb.org/publications/spanish/document/Impacto-de-los-incidentes-de-seguridad-digital-en-Colombia-2017.pdf
[6] OIT Países andinos. 2020. Impacto de la COVID-19 en las Mipymes colombianas. Organización Internacional del Trabajo, Primera edición, Colombia.
https://www.acopi.org.co/wp-content/uploads/2020/12/impacto_covid_web-1.pdf
[7] Usma, A, 2020, Análisis de ciberataques en Colombia durante la cuarentena
https://www.multisoft.com.co/analisis/
[8] Monsalve Mendez, J. Y. 2018. ciberseguridad: principales amenazas en Colombia (ingeniería social, phishing y dos). Bogotá, Colombia. Página: 3-5.
http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4663/00004883.pdf?sequence=1&isAllowed=y
[9] Instituto Nacional de Ciberseguridad (INCIBE). 2020. Guía de ciberataques - Todo lo que debes saber a nivel usuario. España. Página 30.
https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf
[10] Colprensa y El País, 2021. Alerta por aumento de ciberataques en Colombia: van más de mil millones en 2021. Colombia.
https://www.elpais.com.co/judicial/alerta-por-aumento-de-ciberataques-en-colombia-van-mas-de-mil-millones-en-2021.html
[11] López L.H, 2020, Investigar y documentar ataques informáticos más comunes presentados a herramientas de trabajo colaborativo en el contexto organizacional colombiano. UNAD. https://repository.unad.edu.co/handle/10596/40363?locale-attribute=fr
[12] Espinel, S. 2020. Recomendaciones de seguridad para prevención de ciberataques que vulneren la información de los niños, niñas, adolescentes y jóvenes del instituto colombiano para la juventud. https://repository.ucatolica.edu.co/bitstream/10983/25742/1/Trabajo%20de%20Grado%20Sebastian%20Espinel%20Carranza.pdf
[13] Trump, E, 2 de noviembre del 2017. Noticias falsas. Página:5-7.
https://www.palermo.edu/cele/pdf/FakeNews.pdf
[14] González. E. 2018. "Las fake news", la nueva maldición de las empresas.
https://cincodias.elpais.com/cincodias/2018/10/29/companias/1540825299_353052.html
[15] Sicex. 2020. Fake news': enemigo invisible de las empresas en tiempos de crisis. Colombia.
https://sicex.com/blog/fake-news-enemigo-invisible-de-las-empresas-en-tiempos-de-crisis/
[16] Estudio de comunicación - Servimedia. 2018. Influencia de las noticias falsas en la opinión pública.
https://www.servimedia.es/sites/default/files/documentos/informe_sobre_fake_news.pdf
[17] Marín, R, 2020. Cómo prevenir un ciberataque en su negocio y no ser hackeado en el intento. Revista digital Inesem.
https://revistadigital.inesem.es/informatica-y-tics/como-prevenir-un-ciberataque/
[18] Vargas Salcedo, J.C. 2018. Campañas de concientización en seguridad de la información dirigidas a usuarios finales como método de ayuda para la mitigación del riesgo sobre los datos de la empresa. Fundación Universidad Piloto de Colombia. Página 1-12.
http://polux.unipiloto.edu.co:8080/00004663.pdf
[19] Universidad de Jaén, 2018. Guías de seguridad UJA, Phishing. España. https://www.ujaen.es/servicios/sinformatica/sites/servicio_sinformatica/files/uploads/guias-practicas/Guias%20de%20seguridad%20UJA%20-%202.%20Phishing.pdf